P25383

パスワード機能を強化した情報処理システムおよびその情報処理方法
(Information Processing system and method strengthen in Password)

Background of the Invention

Field of the Invention

本発明は、情報処理システムおよびその情報処理方法に関し、特に操作者の利便を高め、かつ、記録された情報のセキュリティを確保する情報処理技術に関するものである。

Description of the Prior Art

近年、情報処理装置が広範囲に使用されるにつれ、情報処理装置本体自体の価値よりも二次記憶装置に記録された情報の価値の方が大きくなってきている。この二次記憶装置は一般には取り外し可能であるので、盗難されると第三者が記録された情報を利用できる危険性がある。このように盗難に遭った場合でも、第三者が二次記憶装置の情報を参照できないようにするセキュリティ技術が求められている。

従来の情報処理装置あるいは情報処理システムでは、盗難後に分解されて二次記憶装置が取り出すことができる。この時、取り出した二次記憶装置を別の情報処理装置に接続して不正使用すれば、起動時のパスワードだけでは情報の不正利用が防げなかった。そこで、従来の情報処理装置においては、二次記憶装置自体にもパスワード（以下、二次パスワードと称す）を設定することにより、二次記憶装置を取り外してもそこに記録された情報が使用できないようにしていた。

しかしながら、従来の情報処理装置あるいは情報処理システムにおいては、起動時に、操作の煩わしさのために、操作者はパスワードを起動用に設定しないことがしばしば有った。また、二次記憶装置用のパスワードを設定しないことが、しばしば有った。そのため情報漏洩の危険性が大きかった。

一方、通常のキーボードを接続せずに、情報処理装置と表示装置の組み合わ

せだけで、情報記処理装置を活用する事がしばしばある。例えば、銀行店頭の自動入出金端末装置や、構内のサービス案内用の端末装置などのように、表示装置と一体となったタッチパネルのような補助的な入力装置により、操作者が簡単に補助的な情報を入力して、必要な情報や案内を利用する場合には通常のキーボードのような入力装置を使わない場合がある。また、販売店の店頭で店の案内や商品の説明を自動的に連続して提示する場合などには、キーボードのような入力装置はもとより、前述のようなタッチパネルさえも使わないことが多い。これら情報処理システムでは、情報処理装置や二次記憶装置に記憶された情報の漏洩を防ぐために、パスワードを事前に設定しておくと、毎回、事前にキーボードから起動用パスワードと二次記憶装置用の二次パスワードを入力する必要がある。それでは、担当者の仕事の能率が上がらない。だからと言って、パスワードの入力手段としてのキーボードが無いと、情報処理装置の起動が不可能であるばかりでなく、二次記憶装置に記憶されている必要な情報の提示さえ行なえない。

本発明は、このように操作者がパスワードを入力するという毎回の煩わしい操作を無くし、かつ、情報処理装置本体や二次記憶装置の盗難時等に情報漏洩の危険性を最小限にすることを目的とする。すなわち、パスワードが設定されていても、パスワード入力が行なえる入力装置が接続されていない場合には、パスワードの有無に関わらず情報処理装置あるいは情報処理システムを起動する。一方、パスワード設定が有る場合には、基の入力装置や別の入力装置でパスワードを正しく入力した時にのみ、情報処理装置あるいは情報処理システムを起動する。このようにして、こ操作者の利便性の向上を図る一方で、情報の不正利用を防ぐ。

Summary of the Invention

上記課題を解決するために本発明による情報処理システムは、

（ａ）情報処理装置本体と、

（b）情報処理装置本体から取り外し可能で、かつ、情報処理装置本体を起動するための起動パスワードを設定する入力手段と、

（c）入力手段で設定した起動パスワードを記憶する起動パスワード記憶手段と、

（d）起動パスワード記憶手段に前記起動パスワードが記憶されているか否かを判定する起動パスワード有無判定手段と、および、

（e）操作者に起動パスワードの設定を要求する起動パスワード要求手段とを有し、

ｉ）入力手段が前記情報処理装置本体に接続されている場合で、かつ、起動パスワード有無判定手段の判定結果が起動パスワード無しの場合には、起動パスワード要求手段により、入力手段による本体の起動に対する起動パスワード設定を要求し、

ｉｉ）入力手段が情報処理装置本体に接続されている場合で、かつ、起動パスワード有無判定手段の判定結果が起動パスワード有りの場合には、情報処理装置本体を起動状態にし、また、

ｉｉｉ）入力手段が情報処理装置本体に接続されていない場合には、前記起動パスワード有無判定手段の判定結果が起動パスワードの有り無しに拘わらず、前記情報処理装置本体を起動状態にする。

また、上記課題を解決するために、情報処理装置本体と前記情報処理装置本体から取り外し可能な入力手段を有する情報処理システムの情報処理方法は、

（a）入力手段で情報処理装置本体を起動するための起動パスワードを設定する、

（b）設定した起動パスワードを記憶する、

（c）前記起動パスワードの記憶の有無を判定する、

（d）操作者に起動パスワード設定を要求する

ステップを備え、

（ｉ）入力手段が情報処理装置本体に接続されている場合で、かつ、ステップ（c）の判定結果が記憶無しの場合には、ステップ（d）を実行

し、

（ｉｉ）入力手段が前記情報処理装置本体に接続されている場合で、かつ、ステップ（ｃ）の判定結果が記憶有りの場合には、前記情報処理装置本体を起動状態にし、

（ｉｉｉ）入力手段が情報処理装置本体に接続されていない場合には、ステップ（ｃ）の判定結果に関わらず、前記情報処理装置本体を起動状態にする。

Brief Description of the Drawings

図１．は本発明に基づく一実施例の情報処理システムのブロック図である。

図２．は本発明に基づくの一実施例における情報処理システムの基本入出力システム（ＢＩＯＳ）の起動時の処理フローチャートである。

Detailed Description of the Preferred Embodiment

以下、本発明の実施の形態について図１～図２を用いて説明する。図１は、本実施例の情報処理システムのブロック図である。

図１において、情報処理システムは、システム全体を制御する中央処理演算装置（ＣＰＵ）１、情報処理システムの電源がＯＮされると情報処理システムの初期化等のために最初に実行されるプログラムである基本入出力システム（ＢＩＯＳ）２、パスワード入力等を行なうための着脱可能な入力装置３，例えば，キーボードなどの入力手段、パスワード入力画面等を表示する表示装置４、パスワード等を保存する不揮発性メモリ５、および、ハードディスク等の二次記憶装置６で構成される。

情報処理装置本体は、一般に、中央処理演算装置（ＣＰＵ）１、基本入出力システム（ＢＩＯＳ）２、パスワード等を保存する不揮発性メモリ５、および、ハードディスクドライブ（ＨＤＤ）等の二次記憶装置６で構成される。

パスワード入力画面等を表示する表示装置４は、例えば、ＣＲＴや液晶表示装置などの表示手段である。これは、情報処理装置本体に一体化されている場合と、情報処理装置本体とは別になっている場合も有る。また、表示装置４は

補助的な情報を入力するタッチパネルのような補助入力手段を含んでいても良い。

二次記憶装置６は、ハードディスクドライブ（ＨＤＤ）以外に、フロッピーディスクドライブ（ＦＤＤ）、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＣＤ－Ｒ／Ｗ、ＣＤ－ＲＡＭ、ＤＶＤ－ＲＯＭ、ＤＶＤ－Ｒ、ＤＶＤ－Ｒ／Ｗ、ＤＶＤ－ＲＡＭ、あるいは、デジタルテープ記録装置などの手段でも良い。しかも、二次記憶装置６は、情報処理装置本体に一体化されている場合と、情報処理装置本体とは別になっていて、取り外し可能場合も有る。また、二次記憶装置６は、情報処理装置本体に一体化されていても、通常、取り外しが出来る。

図２は、本実施の形態における基本入出力システム（ＢＩＯＳ）２の起動時の処理フローチャートである

図２において、電源ＯＮステップ２１は、情報処理システムの電源がＯＮする。すると、情報処理システムは基本入出力システム（ＢＩＯＳ）２を実行開始する。　記録済みパスワードチェックステップ２２は、二次記憶装置６に対する二次パスワードが不揮発性メモリ５と二次記憶装置６とに記憶されているか否かをチェックする。二次パスワードが不揮発性メモリ５と二次記憶装置６とに記憶されていれば、システムの状態は入力装置チェックステップ２４に移る。二次パスワードが不揮発性メモリ５と二次記憶装置６とに記憶されていなければ、システムの状態はパスワード設定画面表示ステップ２３に移って、表示装置４であるＣＲＴや液晶表示装置などの表示手段に二次パスワード設定画面を表示して、操作者に二次パスワードの設定を促す。ここで、このパスワード設定画面表示ステップ２３では、表示装置６が画面表示ではなく、操作者に音声によって二次パスワード設定を促す音声を発生する音声手段であっても良い。

入力装置チェックステップ２４は、入力装置３、例えば、キーボードのような入力手段が情報処理装置本体に接続されているか否かをチェックする。入力装置３が情報処理装置本体に接続されていれば、システムの状態はパスワード入力要求ステップ２５に移る。入力装置３が情報処理装置本体に接続されてい

なければ、システムの状態はパスワード入手ステップ２６に移って、不揮発性メモリ５に記憶されている二次記憶装置６に対する二次パスワードを取得して、システムの状態はパスワードロック解除ステップ２８に移る。　パスワード入力要求ステップ２５は、表示装置４、例えば、ＣＲＴ、液晶表示装置などの表示手段にパスワード入力設定画面を表示する。操作者がパスワード入力設定画面にしたがって、起動パスワードを入力すると、システムの状態は、パスワード一致ステップ２７に移る。

ここで、表示手段に音声手段を用い、音声によって操作者に起動パスワード設定を促すようにしても良い。

パスワード一致ステップ２７は、パスワード入力要求ステップ２５で入力された二次パスワードが不揮発性メモリ５と二次記憶装置６とに記憶されている二次記憶装置６に対する二次パスワードと一致するか否かをチェックする。入力された二次パスワードが不揮発性メモリ５と二次記憶装置６とに記憶されている二次パスワードと一致していれば、システムの状態はパスワードロック解除ステップ２８に移る。入力された二次パスワードが不揮発性メモリ５と二次記憶装置６とに記憶されている二次パスワードと一致していなければ、システムの状態は起動処理中断ステップ２１０に移って、情報処理システム全体あるいは情報処理装置本体の起動処理は中断される。

パスワードロック解除ステップ２８は、パスワード入力要求ステップ２５で入力された起動パスワード、または、パスワード入手ステップ２６で取得した二次パスワードを二次記憶装置６に対して設定する。これにより、システムの状態はパスワードロックを解除して起動処理続行ステップ２９に移り、その結果、情報処理システム全体、あるいは、情報処理装置本体の起動処理は続行される。

二次記憶装置６が取り外され、これが、二次パスワードを設定した情報処理装置本体とは、同じ機種の他の情報処理装置に接続されると、この二次記憶装置６に対する二次パスワードが不揮発性メモリ５と二次記憶装置６とに記憶されているか否かをチェックする。二次パスワードが不揮発性メモリ５と二次記

憶装置６とに記憶されていれば、システムの状態は入力装置チェックステップ２４に移る。二次パスワードが不揮発性メモリ５と二次記憶装置６とに記憶されていなければ、システムの状態はパスワード設定画面表示ステップ２３に移って、表示装置４であるＣＲＴや液晶表示装置などの表示手段に二次パスワード設定画面を表示して、操作者に二次パスワードの設定を促す。ここで不正操作者が、この二次記憶装置６に対する二次パスワードを知らないので、でたらめな起動パスワードやでたらめな二次パスワードしか入力出来ない。すると，入力されたでたらめな二次パスワードが不揮発性メモリ５と二次記憶装置６とに記憶されている二次パスワードと一致しない。したがって、システムの状態は、起動処理中断ステップ２１０に移って、情報処理システム全体あるいは情報処理装置本体の起動処理を中断する。その結果、取り外された二次記憶装置に保存された情報が保護される。

また、情報処理装置本体と二次記憶装置６とが一緒に取り外され、元の物とは別の表示装置に接続された時、入力装置が接続されない限り、二次記憶装置６に記憶されている情報そのものはこの別の表示装置で見ることが出来る。しかしながら、二次記憶装置６に記憶されている情報そのものは改ざん出来ないし、また、他の目的や方法で利用出来ない。このことは前述の説明から明らかであるので、詳しい説明は省略する。

以上詳述したように、本発明の情報処理システムは、入力装置３が情報処理装置に接続されていない時には、情報処理装置が自動的に起動し、二次記憶装置６に記憶した情報が表示装置４に自動的に提示されるので、操作者が使う度に毎回パスワードを入力するという煩わしさは無い。しかも、情報処理装置や二次記憶装置の盗難時等に情報漏洩の危険性を最小限にすることが出来る。すなわち、パスワード設定が有ればパスワード入力が行なえる入力装置が接続されていない場合には、パスワードの有無に関わらず情報記憶装置を起動し、かつ、二次記憶装置の情報を表示装置に提示して、操作者の利便を高める。しかも、起動時や二次記憶装置に対するパスワードの設定が無ければ起動や二次記憶装置のパスワード保護解除をしないようにすることにより、二次記憶装置に

記憶された情報に対するセキュリティを向上することができる。また、パスワード設定が有る場合には、別の入力装置でパスワードを正しく入力した時にのみ、情報記憶装置を起動し、かつ、二次記憶装置の情報を表示装置に提示できるようにすることになるので、情報漏洩の可能性を小さく出来る。